

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-283491

(43)Date of publication of application : 03.10.2003

(51)Int.Cl.

H04L 9/32

G09C 1/00

(21)Application number : 2002-080392

(71)Applicant : HITACHI LTD

(22)Date of filing : 22.03.2002

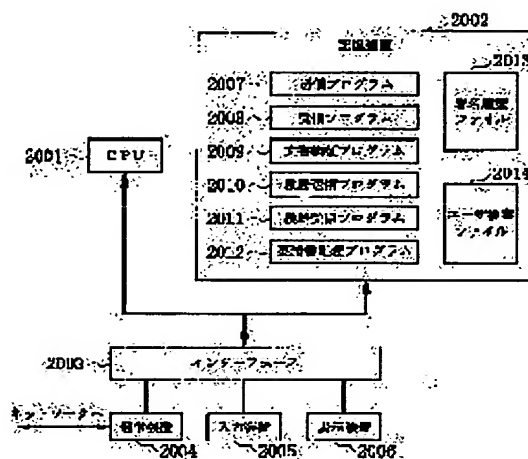
(72)Inventor : TANIMOTO KOICHI
ITO SHINJI
MIYAZAKI KUNHIKO
OMOTO CHIKAHIRO
NISHIOKA KAZUKO

(54) DIGITAL SIGNATURE SYSTEM, DIGITAL SIGNATURE PROCESSOR, PROGRAM AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To efficiently realize a digital signature with high admissibility using a signature history and cross referencing the signature histories by protecting the privacy of the respective users in the case of chained verification.

SOLUTION: Signature numbers (record identification sequential numbers), created signatures and hush values of the previous signature generation records to be used for verification of the chain of the signatures are left as generation records of the respective signatures in a signature history file 2013. In addition, in order to cross reference the signature histories, the signature history file 2013 is updated also in reception of a document with signatures. Furthermore, parties of transmission/reception of the document with signatures are in a user retrieval file 2014 with the signature numbers in the case of updating the signature history records, to what user they are transmitted or from what user they are received are investigated based on the user retrieval file 2014 in the case of cross referencing the signature histories.



LEGAL STATUS

[Date of request for examination] 11.03.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-283491

(P2003-283491A)

(43) 公開日 平成15年10月3日 (2003.10.3)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 L 9/32		G 0 9 C 1/00	6 4 0 D 5 J 1 0 4
G 0 9 C 1/00	6 4 0		6 4 0 E
		H 0 4 L 9/00	6 7 5 B

審査請求 未請求 請求項の数14 O L (全 16 頁)

(21) 出願番号 特願2002-80392(P2002-80392)

(22) 出願日 平成14年3月22日 (2002.3.22)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 谷本 幸一

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72) 発明者 伊藤 信治

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74) 代理人 100077274

弁理士 磯村 雅俊 (外1名)

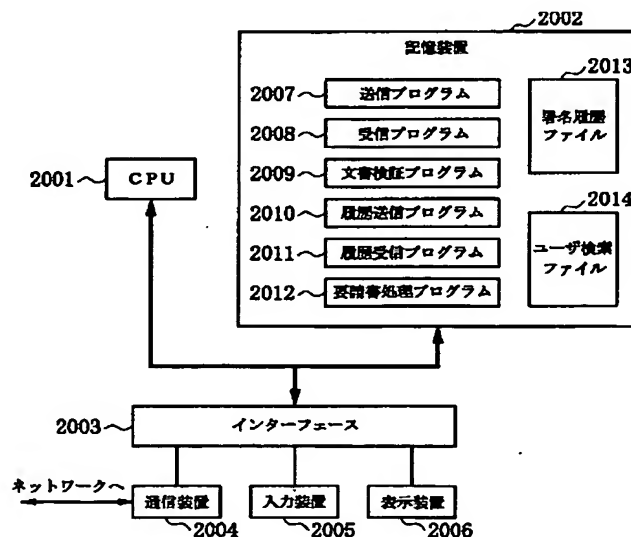
最終頁に続く

(54) 【発明の名称】 デジタル署名管理方法とデジタル署名処理装置およびプログラムと記録媒体

(57) 【要約】

【課題】 連鎖の検証の際の各ユーザのプライバシーを保護して、署名履歴を用いた証拠性の高いデジタル署名、ならびに署名履歴交差を効率的に実現する。

【解決手段】 署名履歴ファイル2013中の各署名生成記録として、署名番号(レコード識別用連番)と、作成した署名、および、履歴の連鎖の検証に用いる前回の署名生成記録のハッシュ値を残す。また、署名履歴交差を実現するために、署名付き文書受信時にも署名履歴ファイル2013を更新する。さらに、ユーザ検索ファイル2014に、署名履歴ファイル2013の更新時に、署名付き文書の送受信相手を署名番号とともに保存し、署名履歴交差利用時、ユーザ検索ファイル2014に基づき、各署名生成記録について、どのユーザに送信、もしくはどのユーザから受信した署名に対するものであるかを調べる。



【特許請求の範囲】

【請求項 1】 送信対象のメッセージに対するデジタル署名の生成に、過去のデジタル署名の生成記録情報を反映させ、生成する全てのデジタル署名に連鎖構造を持たせると共に、受信したメッセージに対する送信元のデジタル署名生成記録情報を生成して署名履歴交差を行うデジタル署名システムにおけるデジタル署名管理方法であって、メッセージとデジタル署名と共に受信した当該デジタル署名の検証用のデータを用いて、当該メッセージに対する送信元のデジタル署名生成記録情報を生成し、上記過去のデジタル署名の生成記録情報として、記憶装置に記憶された署名履歴ファイルに登録する手順と、上記署名履歴ファイルに登録した各デジタル署名生成記録情報に対応付けて、当該デジタル署名生成記録情報が送信時もしくは受信時のいずれの際に生成されたかを示す情報と、当該デジタル署名生成記録情報の生成元メッセージの送信先もしくは送信元の識別情報とを、記憶装置に記憶されたユーザ検索ファイルに登録する手順と、上記ユーザ検索ファイルに登録された情報に基づき、上記署名履歴ファイルから、署名履歴交差に用いるデジタル署名生成記録情報を特定する手順とを有することを特徴とするデジタル署名管理方法。

【請求項 2】 請求項 1 記載のデジタル署名管理方法であって、送信対象のメッセージあるいはそのハッシュ値と、前回登録したデジタル署名生成記録情報のハッシュ値と、今回登録するデジタル署名生成記録情報の識別情報とを結合したデータに、秘密鍵を作用させて当該メッセージに対するデジタル署名を生成する手順を有することを特徴とするデジタル署名管理方法。

【請求項 3】 請求項 1、もしくは、請求項 2 のいずれかに記載のデジタル署名管理方法であって、新たなメッセージの送信に伴い上記署名履歴ファイルにデジタル署名生成記録情報を追加登録する際、追加登録するデジタル署名生成記録情報の識別情報と、上記新たなメッセージの送信に対応して生成したデジタル署名と、上記署名履歴ファイルに前回登録したデジタル署名生成記録情報のハッシュ値とを結合して上記署名履歴ファイルに追加登録するデジタル署名生成記録情報を生成し、該生成したデジタル署名生成記録情報を上記署名履歴ファイルに追加登録する手順を有することを特徴とするデジタル署名管理方法。

【請求項 4】 請求項 1 から請求項 3 のいずれかに記載のデジタル署名管理方法であって、上記送信対象のメッセージと共に、該メッセージに対して作成したデジタル署名と、該デジタル署名を含む上記デジタル署名生成記録情報の識別情報と、上記署名履歴ファイルに前回登録したデジタル署名生成記録情報のハッシュ値とからなる署名データを送信する手順を有することを特徴とするデジタル署名管理方法。

【請求項 5】 請求項 1 から請求項 4 のいずれかに記載のデジタル署名管理方法であって、新たなメッセージの受信に対応したデジタル署名生成記録情報を上記署名履歴ファイルに追加登録する際、追加登録するデジタル署名生成記録情報の識別情報と、上記署名履歴ファイルに前回登録したデジタル署名生成記録情報のハッシュ値と、上記新たなメッセージと共に送信側で生成され送られてきた該メッセージに対するデジタル署名および該デジタル署名を含む上記デジタル署名生成記録情報の識別情報ならびに送信側の署名履歴ファイルにおける前回登録分のデジタル署名生成記録情報のハッシュ値からなる署名データとを結合して、上記署名履歴ファイルに追加登録するデジタル署名生成記録情報を生成し、該生成したデジタル署名生成記録情報を上記署名履歴ファイルに追加登録する手順を有することを特徴とするデジタル署名管理方法。

【請求項 6】 請求項 5 に記載のデジタル署名管理方法であって、受信したメッセージが、該メッセージと共に受信したデジタル署名の生成者から送信されたものであるかを、該デジタル署名の生成者が当該デジタル署名の生成に用いた秘密鍵と対の公開鍵を用いて検証する手順と、過去にメッセージと共に生成あるいは受信したデジタル署名の内、検査対象に指定された検査対象デジタル署名に対応するデジタル署名生成記録情報が、上記署名履歴ファイルに登録されているか否かを検証する手順と、上記署名履歴ファイルに登録されている上記検査対象デジタル署名に対応するデジタル署名生成記録情報まで、該署名履歴ファイルに登録され正当性が確認されている署名生成記録情報を起点として、連鎖の検証を行う手順とを有することを特徴とするデジタル署名管理方法。

【請求項 7】 請求項 1 から請求項 6 のいずれかに記載のデジタル署名管理方法であって、上記署名履歴ファイルに登録したデジタル署名生成記録情報を、上記メッセージの送信と同様の手順で送信して上記署名履歴ファイルの更新を行う手順と、送られてきた上記デジタル署名生成記録情報を、上記メッセージの受信と同様の手順で受信して上記署名履歴ファイルの更新を行う手順とを有することを特徴とするデジタル署名管理方法。

【請求項 8】 請求項 1 から請求項 7 のいずれかに記載のデジタル署名管理方法であって、検証対象デジタル署名の連鎖検証に必要なデジタル署名生成記録情報が上記署名履歴ファイルに無い場合、上記ユーザ検索ファイルを検索して、連鎖検証に利用するデジタル署名生成記録情報の送信先を特定し、特定した送信先に、上記利用するデジタル署名生成記録情報の識別情報を通知して当該デジタル署名生成記録情報の返送を要請する手順と、上記デジタル署名生成記録情報の返送の要請を受けた場合、上記ユーザ検索ファイルを検索して、要請元の特定と該要請元から過去に受信した各デジタ

ル署名生成記録情報の識別情報の特定とを行い、該特定した識別情報と上記要請元から通知された上記利用するデジタル署名生成記録情報の識別情報とに基づき、上記署名履歴ファイルに登録した、上記要請元から通知された上記利用するデジタル署名生成記録情報を特定し、該特定した上記利用するデジタル署名生成記録情報の連鎖検証に用いるデジタル署名生成記録情報を選択して、上記利用するデジタル署名生成記録情報と共に要請元に送信する手順とを有することを特徴とするデジタル署名管理方法。

【請求項 9】 請求項 1 から請求項 8 のいずれかに記載のデジタル署名管理方法であって、メッセージの検証の要望を、調停機関装置に行う際、該調停機関装置に、検証対象のメッセージに関わる署名履歴ファイルを提出する手順を有し、該調停機関装置において、上記署名履歴ファイルを用いて検証を行うことを特徴とするデジタル署名管理方法。

【請求項 10】 請求項 9 に記載のデジタル署名管理方法であって、メッセージの検証の要望を、上記調停機関装置に行う際、該調停機関装置に、検証対象のメッセージに関わる署名履歴ファイルに加えて、さらにユーザ検索ファイルを提出する手順を有し、上記調停機関装置において、上記署名履歴ファイルと上記ユーザ検索ファイルを用いて検証を行うことを特徴とするデジタル署名管理方法。

【請求項 11】 請求項 1 から請求項 10 のいずれかに記載のデジタル署名管理方法であって、上記署名履歴ファイルに登録した最新のデジタル署名生成記録情報を、公開機関装置に、定期的もしくは定数回毎に送信する手順を有し、該公開機関装置において、受信したデジタル署名生成記録情報を審査して公開することを特徴とするデジタル署名管理方法。

【請求項 12】 送信対象のメッセージに対するデジタル署名の生成に、過去のデジタル署名の生成記録情報を反映させ、生成する全てのデジタル署名に連鎖構造を持たせると共に、受信したメッセージに対する送信元のデジタル署名生成記録情報を生成して署名履歴交差を行うデジタル署名処理装置であって、請求項 1 から請求項 11 のいずれかに記載のデジタル署名管理方法における各手順を実行する各機能を有することを特徴とするデジタル署名処理装置。

【請求項 13】 コンピュータに、請求項 1 から請求項 11 のいずれかに記載のデジタル署名管理方法における各手順を実行させるためのプログラム。

【請求項 14】 コンピュータに、請求項 1 から請求項 11 のいずれかに記載のデジタル署名管理方法における各手順を実行させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル署名技術に係わり、特に、デジタル署名の証拠性を高めるのに好適なデジタル署名技術に関するものである。

【0002】

【従来の技術】ネットワークを介しての電子商取引やオンラインショッピング等においては、そのデータ（メッセージ、文書）が特定の送信者が送信したデータであることを証明し、いわゆる「なりすまし」を防止するために、デジタル署名（電子署名）技術が利用されている。

【0003】このデジタル署名（電子署名）では、例えば文書（メッセージ）のハッシュ値で当該文書（メッセージ）の中身を保証し、文書（メッセージ）の改竄を防止できる。

【0004】また、このようなデジタル署名の証拠性を高める従来技術として、例えば、特開 2001-331104 号公報、および、特開 2001-331105 号公報に記載の技術がある。

【0005】これらの公知文献には、署名作成の際、その時点までの署名履歴情報を反映させる技術が記載されている。すなわち、この技術では、作成した署名の署名情報を、作成する毎に、新たに署名履歴に追加する。これにより、作成した全ての署名は連鎖構造を持ち、検証の際は、署名に対する検証の他に、連鎖の検証も行うので、改竄は困難となる。

【0006】上記特開 2001-331104 号公報においては、さらに証拠性を高めるための技術として、

「署名履歴交差」技術が記載されている。この「署名履歴交差」技術は、相手から送られてきた署名に対して、署名履歴情報を作成し、これによって相手の署名情報を自分の署名履歴に取り込むというものである。

【0007】この処理を双方が行うことによって、署名作成時点までの互いの署名履歴が相手の署名履歴に格納され、後に、自分の署名履歴が欠如してしまった場合においても、相手側の署名履歴に残されている自分の署名記録を用いて補うことができる。

【0008】しかし、これらの公知文献においては、署名履歴にどのような情報を残せば良いのか、また、署名履歴交差は実際にはどのようにやれば良いか、その具体的な実現手法は開示されていない。また、連鎖の検証の際に署名履歴が必要なことから、署名履歴が、自分以外の他人に公開されることがある。

【0009】

【発明が解決しようとする課題】解決しようとする問題は、従来の技術では、署名履歴としてどのような情報を残せば良いのか、また、署名履歴交差は実際にはどのようにやれば良いか、その具体的な実現手法が開示されていない点と、署名履歴を利用したデジタル署名においては、連鎖の検証の際に署名履歴が必要なことから、署名履歴が、自分以外の他人に公開されることがある点

である。

【0010】本発明の目的は、これら従来技術の課題を解決し、各ユーザのプライバシーを保護しながら、なおかつ、署名履歴を用いた証拠性の高いデジタル署名、ならびに署名履歴交差を効率的に実現することである。

【0011】

【課題を解決するための手段】上記目的を達成するため、本発明では、効率的な署名履歴交差を実現するために、「ユーザ検索ファイル」を新たに用意する。このユーザ検索ファイルには、署名履歴更新時に、署名付き文書の送受信相手を、署名履歴ファイルとの対応付けに用いる各デジタル署名生成記録情報の識別情報（「署名番号」）とともに保存する。これにより、署名履歴交差利用時には、このユーザ検索ファイルを用いて、各デジタル署名生成記録情報について、どのユーザに送信、もしくはどのユーザから受信した署名に対するものであるかを調べることができる。

【0012】尚、署名履歴ファイルに登録する各デジタル署名生成記録情報は、当該デジタル署名生成記録情報を特定するための識別情報（「署名番号」）と、「作成したデジタル署名」、および、「前回生成したデジタル署名生成記録情報のハッシュ値」からなり、このデジタル署名生成記録情報は、デジタル署名が作成されるたびに、そのデジタル署名に対応して生成され、署名履歴ファイルに追加される。「前回生成したデジタル署名生成記録情報のハッシュ値」は、履歴の連鎖を検証するのに用いる。

【0013】さらに、効率的な署名履歴交差を実現するために、デジタル署名付き文書の受信時にも署名履歴ファイルを更新する。すなわち、受信したデジタル署名と、デジタル署名と共に送られてきたデータ（「署名番号」、「前回生成したデジタル署名生成記録情報のハッシュ値」）から、相手のデジタル署名生成記録情報を作成し、「署名番号」、相手の「デジタル署名生成記録情報のハッシュ値」、および「前回生成したデジタル署名生成記録情報のハッシュ値」をデジタル署名生成記録情報として新たに署名履歴ファイルに追加する。これにより、デジタル署名付き文書の送信時には、そのデジタル署名に対応した自分のデジタル署名生成記録情報が相手の署名履歴ファイルの中にも保存されることになる。

【0014】

【発明の実施の形態】以下、本発明の実施の形態を、図面により詳細に説明する。

【0015】図1は、本発明に係わるデジタル署名システムの構成例を示すブロック図であり、図2は、図1におけるユーザ装置の構成例を示すブロック図、図3は、図2におけるユーザ装置で記憶される署名情報ファイルとユーザ検索ファイルの構成例を示す説明図である。

【0016】図1におけるデジタル署名システムは、複数のユーザ装置1a～1cと、公開機関装置2、および、調停機関装置3のそれぞれをネットワーク4を介して接続した構成である。

【0017】各装置（1a～1c、2、3）は、それぞれ、CPU（Central Processing Unit）や主メモリ、表示装置、入力装置、外部記憶装置等を有したコンピュータ構成からなり、光ディスク駆動装置等を介してCD-ROM等の記憶媒体に記録されたプログラムやデータを外部記憶装置内にインストールした後、この外部記憶装置から主メモリに読み込みCPUで処理することにより、各処理機能を実行している。

【0018】例えば、ユーザ装置1aで代表して示す本発明に係わるデジタル署名処理部5における各処理部（送信処理部5a、受信処理部5b、文書検証処理部5c、履歴送信処理部5d、履歴受信処理部5e、要請書処理部5f）は、図2に示す各プログラム（2007～2012）のそれぞれに基づくCPUの処理により、各機能が実現される。

【0019】ユーザ装置1a～1cは、このデジタル署名処理部5により、本発明に係わるデジタル署名処理装置として、デジタル署名付き文書を送受信する。また、公開機関装置2は、各ユーザ装置1a～1cから定期的に送られてくるデジタル署名生成記録情報（以下「署名生成記録」と記載）を審査・公開する。さらに、調停機関装置3は、各ユーザ装置1a～1cの利用者（ユーザ）間で解決できなかったデータ（メッセージ、文書）の正当性を調査・判定する。

【0020】デジタル署名処理装置としてのユーザ装置1a～1cは、図2に示す構成からなり、本例のデジタル署名システムにおいて、デジタル署名（以下「署名」と記載）を作成したり、署名付き文書や署名履歴を送受信したり、署名付き文書の検証を行う。

【0021】図2に示すように、ユーザ装置1a～1cは、図1におけるデジタル署名処理部5における各機能（送信処理部5a、受信処理部5b、文書検証処理部5c、履歴送信処理部5d、履歴受信処理部5e、要請書処理部5f）を実現するための各種プログラム（2007～2012）と署名履歴2013とユーザ検索ファイル2014が格納されている記憶装置2002と、ネットワーク4を介して他の装置と通信を行うための通信装置2004と、キーボードやマウスなどの入力装置2005と、ディスプレイなどの表示装置2006と、CPU2001とから構築されている。

【0022】CPU2001は、インターフェース2003を介して記憶装置2002から読み出した各プログラム（送信プログラム2007、受信プログラム2008、文書検証プログラム2009、履歴送信プログラム2010、履歴受信プログラム2011、要請書処理プログラム2012）に基づき、署名の作成や検証、署名

履歴ファイル2013の読み込みや更新、ユーザ検索ファイル2014の読み込みや更新を行う。

【0023】本例においては、文書の検証には、「署名のみを使った検証」と、「自分（署名付き文書作成者）の署名履歴を使った検証」、および、「他人の署名履歴を使った検証（署名履歴交差）」とがある。

【0024】例えば、署名に使用する暗号方式が破られていない場合は、「署名のみを使った検証」で良い。しかしながら、暗号方式が破られた場合や、署名に使った秘密鍵が漏洩した、もしくはその恐れがある場合、また、より確かな検証を行いたい場合は、「自分の署名履歴を使った検証」も行う。さらに、この「自分の署名履歴」が欠如等した場合には、「他人の署名履歴を使った検証」を行う。

【0025】また、各ユーザ装置1a～1cは、定期的もしくは定数回毎に最新の署名生成記録を公開機関装置2に送信する。これは、公開機関によって署名生成記録を公開してもらうことにより、その署名生成記録が正当なものであることを示すことを目的とする。

【0026】公開機関装置2は、各ユーザ装置1a～1cから受信した署名生成記録の身元を審査し、一般に公開する。公開することにより、正当な署名作成者以外が作成した署名生成記録が不正であることは、正当な署名作成者の指摘により発覚するため、公開した署名生成記録は、正当な署名生成記録であるものとして扱うことができる。

【0027】尚、公開機関に公開する代わりに、新聞などに公開することによっても、公開した署名生成記録が正当なものであることを示すことができる。

【0028】調停機関装置3は、各ユーザ装置1a～1cから文書の正当性の判定の要望があった場合に、検証対象文書に関わる署名履歴ファイル2013や、必要に応じて、ユーザ検索ファイル2014等を提出させ、それを用いて検証を行い、判定する。

【0029】例えば、検証に必要な署名履歴が欠如していた場合、署名履歴交差により他人の署名履歴を利用することになるが、個人の要請では協力してもらえないことも想定できる。その場合、調停機関が代わりに協力要請し、署名履歴を取得して、目的の検証を行う。また、各ユーザ装置1a～1c間で検証を行った文書について、要望に応じてその結果に対する認定を行う。

【0030】図2の構成図にあるように、各ユーザ装置1a～1cでは、送信プログラム2007、受信プログラム2008、文書検証プログラム2009、履歴送信プログラム2010、履歴受信プログラム2011、要請書プログラム2012により、本デジタル署名システムにおける処理が行われる。

【0031】また、各ユーザ装置1a～1cは、署名生成記録を保存するための署名履歴ファイル2013と、送受信相手の情報を保存するためのユーザ検索ファイル

2014とを持ち、それぞれは、図3において示す構成からなる。

【0032】図3(a)に示すように、本例の署名履歴ファイル2013は、「番号」、「前回署名記録のハッシュ値」、「文書のハッシュ値」、「署名or相手の署名生成記録情報」の各項目3004～3007からなるレコード3001～3003で構成され、また、図3(b)に示すように、本例のユーザ検索ファイル2014は、「番号」、「送受信符号」、「相手情報」の各項目3011～3013からなるレコード3008～3010で構成されている。

【0033】署名履歴ファイル2013における項目3004の「番号」は、連番で付与され、署名履歴の中から特定のレコード（「署名生成記録」）を指定するのに用いられる。

【0034】また、項目3005の「前回署名記録のハッシュ値」は、履歴の連鎖を検証するのに用いられるものであり、例えば、番号「2」で指定されるレコード3002における項目3005の「前回署名記録のハッシュ値」の「H(S1)」は、番号「1」で指定されるレコード3001における各項目3004～3007における各値「1」、「H(S0)」、「H(M1)」、「Sign(1||H(S0)||H(M1))」から算出される。

【0035】また、項目3006の「文書のハッシュ値」を署名履歴ファイル2013の項目として残すことにより、当該レコード（「署名生成記録」）を改竄するためには、それに対応する署名の作成対象となった文書が必要となり、改竄がより困難となっている。尚、この項目3006の「文書のハッシュ値」に関しては、署名履歴ファイル2013の項目として残すことは必ずしも必要ではない。

【0036】また、項目3007の「署名or相手の署名生成記録情報」には、自装置での署名生成時には、各項目3004～3006に対して生成した署名記録情報が、また、相手方から署名を受信した際には、相手方で同様な手順で生成された署名記録情報が登録される。

【0037】例えば、レコード3001は、自装置で生成されたものであり、項目3007には、項目3004～3006の各値（「1」、「H(S0)」、「H(M1)」）から生成された署名「Sign(1||H(S0)||H(M1))」が記録されている。

【0038】また、レコード3002は、相手方装置で生成されたものを受信したものであり、項目3007には、相手方装置で生成され送られてきた署名データ（「署名番号」、「前回生成した署名生成記録情報のハッシュ値」、「署名」）から生成した値（「32||H(S32)」）が記録されている。尚、この値「32||H(S32)」における「32」は、相手方装置で記録している署名履歴ファイル（2013）におけるレコー

ド番号（項目3004の「番号」の値）である。

【0039】ユーザ検索ファイル2014は、署名履歴交差を効率的に利用するために設けられ、このユーザ検索ファイル2014には、署名履歴ファイル2013の更新時に、署名付き文書の送受信相手を、「署名番号」とともに保存する。

【0040】例えば、ユーザ検索ファイル2014におけるレコード3008の項目3011の「番号=1」は、署名履歴ファイル2013における項目3004の「番号=1」に対応しており、ユーザ検索ファイル2014における項目3012の「送信」は、署名履歴ファイル2013における項目3004が「番号=1」のレコード3001は、自装置で生成されて次の項目3013で示される相手方、すなわち「kunihiko@AAA.co.jp」に送信されたことを示している。

【0041】これにより、署名履歴交差利用時には、このユーザ検索ファイル2014を用いて、各署名生成記録について、どのユーザに送信、もしくはどのユーザから受信した署名に対するものであるかを調べることができる。

【0042】以下、このような構成からなる各ユーザ装置1a～1cによるデジタル署名システムとしての処理動作を、図4～図9を用いて説明する。

【0043】図4は、図2におけるユーザ装置の送信プログラムに基づく処理動作例を示すフローチャートであり、図5は、図2におけるユーザ装置の受信プログラムに基づく処理動作例を示すフローチャート、図6は、図2におけるユーザ装置の文書検証プログラムに基づく処理動作例を示すフローチャート、図7は、図2におけるユーザ装置の署名履歴送信プログラムに基づく処理動作例を示すフローチャート、図8は、図2におけるユーザ装置の署名履歴受信プログラムに基づく処理動作例を示すフローチャート、図9は、図2におけるユーザ装置の要請書処理プログラムに基づく処理動作例を示すフローチャートである。

【0044】本図4に示す例は、図2におけるユーザ装置の送信プログラム2007に基づく処理動作、すなわち、図1におけるユーザ装置1aのデジタル処理部5の送信処理部5aの処理動作例であり、まず、ステップS4001では、署名を作成する対象となる文書に対してハッシュ関数を適用し、文書のハッシュ値を計算する。

【0045】図3(a)に示す署名履歴ファイル2013の例では、例えば、レコード3003（「番号=3」）における項目3006の「文書のハッシュ値」として「H(M3)」が計算され記録されている。

【0046】次にステップS4002では、署名履歴ファイル（2013）中から、前回署名作成もしくは署名受信時に作成した署名生成記録、すなわち最新の署名生成記録を取り出す。そして、ステップS4003では、

ステップS4002で取り出した最新の署名生成記録に対してハッシュ関数を適用し、そのハッシュ値を計算する。

【0047】例えば、図3(a)に示す署名履歴ファイル2013におけるレコード3002が最新の署名生成記録であるとする、その項目3007における「署名or相手の署名生成記録情報」の「32||H(S2)」に対してハッシュ関数を適用し、そのハッシュ値を計算し、その結果、レコード3003における項目3005の「前回署名記録のハッシュ値」として「H(S2)」が記録される。

【0048】さらにステップS4004では、署名記録番号と、ステップS4001およびステップS4003のそれぞれで得たハッシュ値を結合したデータに対して、秘密鍵を利用してデジタル署名を作成する。

【0049】ここで、署名記録番号とは、各署名生成記録に固有の（連番で付けられる）番号で、各署名生成記録を判別するのに用いる。例えば、今回作成する署名に対応する署名記録番号は、前回の署名生成記録の記録番号に「1」を加えたものであり、図3(a)に示す署名履歴ファイル2013の各レコード3001～3003における項目3004の「番号(1～3)」に相当する。

【0050】そして、このステップS4004でのデジタル署名の作成は、図3(a)の例では、例えばレコード3003で示されるように、署名記録番号「3」と、ステップS4001で得たハッシュ値（「H(M3)」）およびステップS4003で得たハッシュ値（「H(S2)」）を結合したデータに対して、秘密鍵を利用してデジタル署名（「Sign(3||H(S2)||H(M3))」）が作成される。

【0051】尚、この署名記録番号（例えば「3」）は必ずしも署名対象データに加える必要はないが、改竄されると署名履歴交差利用に支障をきたすため、これも含めて署名対象データとするのが望ましい。

【0052】このように、ステップS4004の処理において、ステップS4003で得た前回の署名生成記録のハッシュ値を署名対象データに加えることで、署名対象文書に対して署名履歴を反映させたデジタル署名を生成することができる。

【0053】次のステップS4005では、前述のステップS4004で署名を作成するのに用いたデータ（署名記録番号、前回署名生成記録のハッシュ値、文書のハッシュ値）と、作成した署名とを結合して署名生成記録を生成する。これが今回作成した署名に対応した署名生成記録となり、図3(a)の署名履歴ファイル2013の各レコード3001、3003（レコード3002は除く）で例示する構成で記録、管理される。

【0054】さらに続いてステップS4006において、ユーザ検索ファイル（2014）に、今回作成した

署名に対応する署名記録番号と送信先相手の情報を追加する。尚、送信先相手の情報には、例えば、図3(b)のユーザ検索ファイル2014の項目3013において例示するように、メールアドレスが挙げられる。

【0055】そして、ステップS4007では、当該文書に、ステップS4004で作成した署名と、検証に必要なデータ（署名記録番号、前回署名生成記録のハッシュ値）、検証に必要な公開鍵および公開鍵証明書をつけて送信する。

【0056】次に、図5により、図2におけるユーザ装置の受信プログラム2008に基づく処理動作、すなわち、図1におけるユーザ装置1aのデジタル処理部5の受信処理部5bの処理動作例を説明する。

【0057】まずステップS5001において、デジタル署名付き文書を受信した場合には、ステップS5003以下の処理を行う。

【0058】ステップS5003では、文書とともに送られてきた公開鍵と公開鍵証明書について、正しいものであるか検証を行う。次のステップS5005では、送られてきた文書に対してハッシュ関数を適用してハッシュ値を計算する。

【0059】ステップS5006では、文書とともに送られてきた署名記録番号、前回署名生成記録のハッシュ値と、ステップS5005で作成した文書のハッシュ値、公開鍵を利用して署名の検証を行う。

【0060】検証成功であれば、ステップS5008において、署名生成記録を作成し、署名履歴を更新する。例えば、図3(a)の署名履歴ファイル2013におけるレコード3002（「番号＝2」）に示すようにして新たなレコードを追加する。

【0061】この受信時のレコード3002での署名生成記録は、送信の時とは異なり、文書とともに送られてきたデータから送信元の署名生成記録を作成し、送信時での署名の代わりに、そのハッシュ値（「H(S32)」）を保存する。

【0062】このように、受信時にも相手の署名情報を記録した署名生成記録を作成して履歴（署名履歴ファイル2013）を更新することで、ユーザ間で互いの履歴情報を分散確保するという署名履歴交差を実現し、署名履歴消失などが起こった場合にも、署名履歴交差を利用して対処可能となる。尚、受信時に履歴を更新するかどうかは受信側に毎回選択させても良い。

【0063】ステップS5009では、ユーザ検索ファイル(2014)に、今回受信した署名に対応する署名記録番号と送信元相手の情報を追加する。すなわち、図3(b)のユーザ検索ファイル2014のレコード3009で示すように、その項目3012の「送受信符号」は「受信」として記録され、項目3013の「相手情報」として、送信元のメールアドレス「s-ito@BBB.co.jp」が記録される。

【0064】そして最後に、ステップS5010において、署名付き文書を任意の場所に格納する。

【0065】次に、図6により、図2におけるユーザ装置の文書検証プログラム2009に基づく処理動作、すなわち、図1におけるユーザ装置1aのデジタル処理部5の文書検証処理部5cの処理動作例を説明する。

【0066】この文書検証プログラム2009は、過去に作成もしくは受信した文書について、署名履歴を利用した署名検証を行うものであり、まずステップS6001、S6002において、文書とそれに付けられた署名および検証に必要なデータを利用して、通常の署名検証（図5におけるステップS5003～ステップS5006）を行う。

【0067】次にステップS6003、S6004において、検証対象署名に対応する署名生成記録が、署名履歴中に存在するかどうか、また公開した署名生成記録が署名履歴中に存在するかどうか調べる。ここで使用する署名履歴は、自分の署名履歴ファイル(2013)であるか、または、検証対象署名の署名者の署名履歴であるかのどちらかである。

【0068】署名生成記録の存在を調べる処理は、過去に生成あるいは受信した文書とそのデジタル署名の内、検証対象に指定されたデジタル署名（検証対象デジタル署名）と、その検証対象デジタル署名を生成した時あるいは受信した時に作成して署名履歴ファイル(2013)に登録された署名生成記録情報に含まれる署名データ（デジタル署名と、このデジタル署名を含む署名生成記録情報の番号（識別情報）ならびに前回登録分のデジタル署名生成記録情報のハッシュ値からなる）とが一致しているか照合することで行う。

【0069】さらに、ステップS6005、6006において、公開した署名生成記録と履歴中同じ番号の署名生成記録とを比較して、一致するかどうか調べ、ステップS6007、6008において、検証対象署名と、それに対応する署名生成記録中に保存されている署名とが一致するかどうか調べる。

【0070】そして、ステップS6009～6011では、公開した署名生成記録と同じ番号の署名生成記録を起点として、検証対象署名に対応する署名生成記録まで連鎖を遡って検証する。具体的には、1つ前の署名生成記録のハッシュ値をとったものと、署名生成記録中に残されている前回署名生成記録のハッシュ値との比較を行い、一致すれば2つの署名生成履歴は正しく連鎖が繋がっているものとする。

【0071】最後に、ステップS6011において、検証結果を表示する。

【0072】次に、図7により、図2におけるユーザ装置の署名履歴送信プログラム2010に基づく処理動作、すなわち、図1におけるユーザ装置1aのデジタル処理部5の署名履歴送信処理部5dによる署名履歴を

送信する履歴送信ステップ処理動作例を説明する。まずステップS7001において、送信する署名履歴を署名履歴ファイル(2013)から取得する。

【0073】そして、ステップS7002～ステップS7006において、文書送信の時と同様に、署名履歴に対して署名を作成し、署名履歴ファイル(2013)、ユーザ検索ファイル(2014)を更新する。

【0074】最後に、ステップS7007において、ステップS7001で取得した署名履歴を相手に送信する。ここで、署名者が過去に署名を付けて送信した文書に対して、受信者が受け取った署名付き文書の正当性を文書検証処理によって検証したい場合には、署名者は、受信者の要請に応じて、検証に必要な署名履歴を署名履歴送信プログラム2010に基づき送信する。

【0075】次に、図8により、図2におけるユーザ装置の署名履歴受信プログラム2011に基づく処理動作、すなわち、図1におけるユーザ装置1aのデジタル処理部5の署名履歴受信処理部5eによる署名履歴を受信する履歴受信ステップの処理動作例を説明する。

【0076】この署名履歴受信プログラム2011に基づきユーザ装置は、ステップS8001～ステップS8008において、受け取った署名履歴とそれに付けられた署名について、通常の署名検証を行い、署名履歴ファイル(2013)、ユーザ検索ファイル(2014)の更新を行う。

【0077】そして、ステップS8009において、受信した署名履歴をハードディスク等の記憶装置に格納する。格納した署名履歴は、文書検証処理の際に利用される。

【0078】次に、図9により、図2におけるユーザ装置の要請書処理プログラム2012に基づく処理動作、すなわち、図1におけるユーザ装置1aのデジタル処理部5の要請書処理部5fの処理動作例を説明する。この要請書処理プログラム2012は、署名履歴交差を利用する際に使用する要請書を扱うものである。

【0079】この署名履歴交差は、検証したい署名に対応する署名生成記録以後に公開した署名生成記録が無い場合や、履歴の一部が欠如して連鎖が検証できない場合などに、相手の署名生成記録を利用して検証可能にする技術である。また、要請書は、署名履歴交差を利用した検証に必要な署名生成記録を相手に要請するために使用する文書である。

【0080】署名履歴交差を利用する際には、誰に要請書を送ればよいか決定しなければならない。すなわち、目的の署名の検証を行うためには、自分の署名履歴中どの署名生成記録の正当性が証明できれば良いか調べた後に、その署名生成記録が誰の署名履歴に保存されているかを知らなければならない。

【0081】このように、各署名生成記録がどの署名に対応しているか、すなわち誰に送信した文書に付けた署

名に対応しているか、あるいは誰から受信した署名についてのものであるかを知る技術として、取引相手の情報(例えば、メールアドレス)も署名生成記録に残しておくことが有効である。

【0082】しかしながら、署名履歴は、文書検証を行う際や、署名履歴交差を利用する際に、その一部もしくは全てを他人に渡すため、取引相手の情報が署名生成記録に残っていた場合、それによって誰と取引しているか他人に漏洩してしまう。

【0083】本例では、取引相手の情報を、署名履歴(2013)とは別のユーザ検索ファイル(2014)に保存し、各署名生成記録とユーザ検索ファイル(2014)中の取引相手情報とは、署名記録番号によるみ対応付けているため、署名履歴を公開もしくは他人に送信した場合であっても、取引相手の情報が漏洩することはない。

【0084】すなわち、ユーザ装置は、要請書処理プログラム2012に基づき、まずステップS9001、S9002において、要請書処理内容が要請書の受信であるか送信であるか判別し、送信であれば、ステップS9003において、検証対象署名の検証が可能となるためにはどの署名生成記録の正当性が証明できれば良いか検索する。

【0085】このステップS9003で検索した検証に必要な署名生成記録について、ステップS9004において、その署名記録番号を参照して、ユーザ検索ファイル(2014)から、検証に必要な署名生成記録が誰のところに保存されているか調べる。

【0086】そして、ステップS9005において、ステップS9004で検索したユーザに対して、必要な署名生成記録の番号を記した要請書を送信する。

【0087】また、ステップS9002の判別結果が、要請書の受信であれば、まず要請書送信元の情報(例えば、メールアドレス)に基づき、ステップS9006において、ユーザ検索ファイル(2014)を検索して、以前に要請書送信元ユーザから文書を受信した際に生成した署名生成記録を探す。

【0088】次に、ステップS9007において、ステップS9006で検索した署名生成記録の中から、要請書に記載されている署名記録番号(相手が必要とする署名生成記録の番号)に該当する相手の署名生成記録が保存されている署名生成記録を抽出する。

【0089】そして、ステップS9008において、要請書送信元が目的の署名を検証するために必要な署名生成記録を求める。具体的には、ステップS9007で抽出した署名生成記録以後に公開した署名生成記録を見つけ、ステップS9007で抽出した署名生成記録から、公開した署名生成記録までの全ての署名生成記録を、相手が検証に必要な署名生成記録とする。

【0090】最後に、ステップS9009において、ス

テップ S9008 で求めた署名生成記録を要請書送信元へ送信する。

【0091】このような、要請書送信者と要請書受信者が署名履歴交差を利用する際の手順について、図10を用いて、より具体的に説明する。

【0092】図10は、本発明に係わるデジタル署名システムの処理動作の具体例を示す説明図である。

【0093】本図10における例では、ユーザ装置Aは、Aの署名履歴10001中、署名記録番号「27」に対応する署名を検証したいが、署名生成記録番号「31」以降の履歴が欠如してしまい、このままでは署名を検証することができない。しかしながら、本例によれば、以下のように署名履歴交差を利用することにより、署名の検証が可能となる。

【0094】ユーザ装置Aは、署名記録番号「27～31」の間で、ユーザ装置Aの署名生成記録が保存されている可能性のある相手を、Aのユーザ検索ファイル10002を用いて検索する。

【0095】その結果、例えば、記録番号「30」の署名生成記録は、ユーザ装置Bに署名付き文書を送信する際に生成した署名の署名生成記録であるから、ユーザ装置Bの署名履歴にはユーザ装置Aの「30」番の署名生成記録が保管されていることが分かる（図中「(1)」）。

【0096】そこで、ユーザ装置Aは、署名記録番号「30」の署名生成記録が必要であるという内容の要請書10003を作成し、ユーザ装置Bに送信する（図中「(2)」）。

【0097】このように、本例では、要請書の送受信によって、検証に必要な署名履歴を相手に伝え、協力を要請する。これにより署名履歴交差を利用した検証を実現する。

【0098】すなわち、要請者ユーザ装置Aから要請書10003を受け取ったユーザ装置Bは、Bのユーザ検索ファイル10004を用いて、Bの署名履歴10005中、ユーザ装置Aから署名付き文書を受信した時に生成した署名生成記録を検索する。その結果、例えば、Bの署名履歴10005中、署名記録番号「21」と「23」の署名生成記録が該当署名記録であることがわかる（図中「(3)」）。

【0099】ユーザ装置Bでは、Bの署名履歴10005中、記録番号「21」と「23」の署名生成記録を調べることにより、例えば、ユーザ装置Aが必要とするユーザ装置Aの「30」番の署名生成記録を保存している署名生成記録は、「21」番の署名生成記録であると特定できる。

【0100】本図10において、Bの署名履歴10005中の「24」番の署名生成記録は、図1における公開機関装置2で公開しているので、「21」～「24」番の署名生成記録をユーザ装置Bからユーザ装置Aに送信

すれば、ユーザ装置Aは、ユーザ装置Bから送られてきた署名履歴を用いて目的の署名を検証することができる。そこで、ユーザ装置Bは、「21」～「24」番の署名生成記録をユーザ装置Aに送信する（図中「(4)」）。

【0101】ユーザ装置Aは、ユーザ装置Bから送られてきた「21」～「24」番の署名生成記録を用いて目的の署名（「27」）を検証する。

【0102】以上、図1～図10を用いて説明したように、本例では、署名履歴ファイル2013中の各署名生成記録（デジタル署名生成記録情報）には、署名番号（識別情報）と、作成した署名（デジタル署名）、および、前回の署名生成記録のハッシュ値を残す。ここで署名生成記録（デジタル署名生成記録情報）とは、履歴（署名履歴ファイル2013）に残すために各署名（デジタル署名）作成時に生成する署名情報であり、署名（デジタル署名）が作成されるたびに、その署名に対応した署名生成記録が生成され、履歴（署名履歴ファイル2013）に追加される。また、「署名番号」（識別情報）は、連番で付加し、署名履歴の中から特定の署名生成記録（デジタル署名生成記録情報）を指定するのに用いる。また、作成した署名（デジタル署名）は、署名生成記録（デジタル署名生成記録情報）とそれに対応する署名との関係が正しいことを証明する。そして、前回の署名生成記録のハッシュ値は、履歴の連鎖を検証するのに用いる。

【0103】さらに、本例では、署名履歴交差を実現するために、署名付き文書受信時にも署名履歴ファイル2013を更新する。すなわち、署名とともに送られてきたデータから、相手の署名生成記録（デジタル署名生成記録情報）を作成し、署名番号（識別情報）、相手の署名生成記録（デジタル署名生成記録情報）のハッシュ値、前回の署名生成記録（デジタル署名生成記録情報）のハッシュ値を、今回の署名生成記録（デジタル署名生成記録情報）として新たに履歴（署名履歴ファイル2013）に追加する。これにより、署名付き文書の送信時には、その署名（デジタル署名）に対応した自分の署名生成記録（デジタル署名生成記録情報）が相手の署名履歴（署名履歴ファイル2013）の中にも保存されることになる。

【0104】そして、より効率的な署名履歴交差を実現するために、ユーザ検索ファイル2014を新たに用意する。このユーザ検索ファイル2014には、署名履歴（署名履歴ファイル2013）の更新時に、デジタル署名付きデータ（メッセージ、文書）の送受信相手を、署名番号（識別情報）とともに保存する。これにより、署名履歴交差の利用時には、ユーザ検索ファイル2014を用いて、各署名生成記録（デジタル署名生成記録情報）について、どのユーザに送信、もしくはどのユーザから受信した署名に対するものであるかを調べるこ

ができる。

【0105】すなわち、本例では、デジタル署名生成側のユーザ装置において、メッセージあるいはそのハッシュ値に、デジタル署名生成者が有する秘密鍵を作用させ、当該メッセージに対するデジタル署名を生成する署名生成処理と、生成したデジタル署名から、その署名情報を記録した署名生成記録（デジタル署名生成記録情報）を生成し、過去に生成された署名生成記録が登録されている署名履歴（署名履歴ファイル2013）に新たに生成した署名生成記録を追加する署名履歴更新処理と、生成したデジタル署名とメッセージを含むデジタル署名付きメッセージを送信する送信処理とを行い、また、デジタル署名検証者側のユーザ装置において、送付されたデジタル署名付きメッセージを、検証対象デジタル署名付きメッセージとして受け付ける受信処理と、受信したデジタル署名付きメッセージが、デジタル署名生成者により送付されたものであるかを、秘密鍵と対の公開鍵を用いてメッセージとデジタル署名が正しく対応しているかを調べることにより検証する検証処理と、受信したデジタル署名から、その署名情報を記録した署名生成記録を生成し、過去に生成された署名生成記録が登録されている署名履歴（署名履歴ファイル2013）に新たに生成した署名生成記録を追加する署名履歴更新処理とを行う。

【0106】また、デジタル署名生成側での署名生成処理は、メッセージあるいはそのハッシュ値と、前回署名作成時あるいは受信時に記録された署名生成記録のハッシュ値と、作成した署名生成記録の中から特定の署名生成記録を識別するために署名生成記録ごとに付けられた署名記録番号（識別情報）とを結合した署名対象データに、秘密鍵を作用させて、当該メッセージに対するデジタル署名を生成する。

【0107】また、デジタル署名生成側での署名履歴更新処理は、作成した署名生成記録の中から特定の署名生成記録を識別するために署名生成記録ごとに付けられた署名記録番号（識別情報）と、作成した署名と、前回署名作成時あるいは受信時に生成した署名生成記録のハッシュ値とを結合して、今回生成した署名に対する署名生成記録を作成し、過去に生成された署名生成記録が登録されている署名履歴（署名履歴ファイル2013）に、今回、新たに生成した署名生成記録を追加する。

【0108】また、履歴更新処理では、署名履歴の更新に加えて、各署名付きメッセージの取引相手を記録するために、署名生成時あるいは署名付きメッセージ受信時に、その時生成あるいは受信した署名情報が記録された署名生成記録に固有の署名記録番号（識別情報）と、生成した署名の送信相手あるいは受信した署名の作成者（送信元）のユーザ情報とを記録したユーザ検索ファイル（2014）を更新する。

【0109】また、デジタル署名生成側の送信処理で

は、メッセージと、それに対して作成されたデジタル署名と、デジタル署名に対して作成した署名生成記録の署名記録番号（識別情報）と、前回署名作成時あるいは受信時に記録された署名生成記録のハッシュ値とを送信する。

【0110】また、デジタル署名検証側の署名履歴更新処理では、デジタル署名側より送られてきた署名データと、作成した署名生成記録の中から特定の署名生成記録を識別するために署名生成記録ごとに付けられた署名記録番号（識別情報）と、前回署名作成時あるいは受信時に作成した署名生成記録のハッシュ値とを結合して、今回受信した署名に対する署名生成記録を作成し、過去に生成された署名生成記録が登録されている署名履歴（署名履歴ファイル2013）に、新たに今回作成した署名生成記録を追加する。

【0111】また、デジタル署名検証側の検証処理に加えて、過去に生成あるいは受信した検証対象デジタル署名に対して、その過去に生成あるいは受信した検証対象デジタル署名と、そのデジタル署名を生成した時あるいは受信した時に作成した署名生成記録中に含まれる署名データとが一致しているか検証し、さらに、最新の正当な署名生成記録から検証対象デジタル署名データが含まれる署名生成記録まで署名生成記録の連鎖が正しく繋がっているかを検証する履歴検証処理を行う。

【0112】さらに、署名履歴を送信する履歴送信処理、または、署名履歴を受信する履歴受信処理を行う。

【0113】また、デジタル署名検証者側の装置では、署名履歴を用いた検証を行う際、検証に必要な署名履歴が無い場合、他のユーザの署名履歴を利用するために、検証に必要な署名生成記録の署名記録番号を他のユーザに伝える要請書送信処理を行う。

【0114】また、要請書受信した際、要請書受信側は、要請書記載の要求署名記録に応じて、要請書送信側に、署名履歴の全部もしくは一部を送信する要請書受信処理を行う。

【0115】このような要請書送信先の決定や、履歴送信において送信する履歴の範囲を決定する時には、ユーザ検索ファイル2014に記録された署名記録番号と送受信相手の情報を利用する。

【0116】このように、本例では、署名履歴を利用した、デジタル署名の改竄・偽造がより困難であるデジタル署名技術を提供することができ、また、他人の履歴を用いた検証や、署名生成記録の分散確保により、自分の署名履歴が欠如した場合でも、他人の署名履歴を利用して、欠如を補って検証することができ、より安全性と信頼性の高いデジタル署名技術を実現することができる。

【0117】尚、本発明は、図1～図10を用いて説明した例に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能である。例えば、本例で

は、図1に示すように、各ユーザ装置1a～1cと公開機関装置2、調停機関装置3のそれぞれをネットワークを介して接続した構成としているが、調停機関装置3を用いない構成としても良く、また、新聞等での公開を行うことで、公開機関装置2も用いない構成、すなわち、各ユーザ装置1a～1cからなる構成としても良い。

【0118】また、各ユーザ装置1a～1cに関しても、この3台の構成に限るものではなく、より多くのユーザ装置を設けることでも良い。また、このユーザ装置1a～1cの構成に関しても、図2に示される構成に限るものではなく、例えば、マイクや音声変換機能等を設けて、音声データを対象としてデジタル署名を施す構成としても良い。

【0119】また、本例では、光ディスクをプログラムの記録媒体として用いているが、FD (Flexible Disk) 等を記録媒体として用いることでも良い。また、プログラムのインストールに関しても、通信装置を介してネットワーク経由でプログラムをダウンロードしてインストールすることでも良い。

【0120】

【発明の効果】本発明によれば、連鎖の検証の際にも、署名履歴が、自分以外の他人に公開されることがなく、各ユーザのプライバシーを保護しながら、なおかつ、署名履歴を用いた証拠性の高いデジタル署名、ならびに署名履歴交差を効率的に実現することが可能である。

【図面の簡単な説明】

【図1】本発明に係わるデジタル署名システムの構成例を示すブロック図である。

【図2】図1におけるユーザ装置の構成例を示すブロック図である。

【図3】図2におけるユーザ装置で記憶される署名情報ファイルとユーザ検索ファイルの構成例を示す説明図である。

【図4】図2におけるユーザ装置の送信プログラムに基

づく処理動作例を示すフローチャートである。

【図5】図2におけるユーザ装置の受信プログラムに基づく処理動作例を示すフローチャートである。

【図6】図2におけるユーザ装置の文書検証プログラムに基づく処理動作例を示すフローチャートである。

【図7】図2におけるユーザ装置の署名履歴送信プログラムに基づく処理動作例を示すフローチャートである。

【図8】図2におけるユーザ装置の署名履歴受信プログラムに基づく処理動作例を示すフローチャートである。

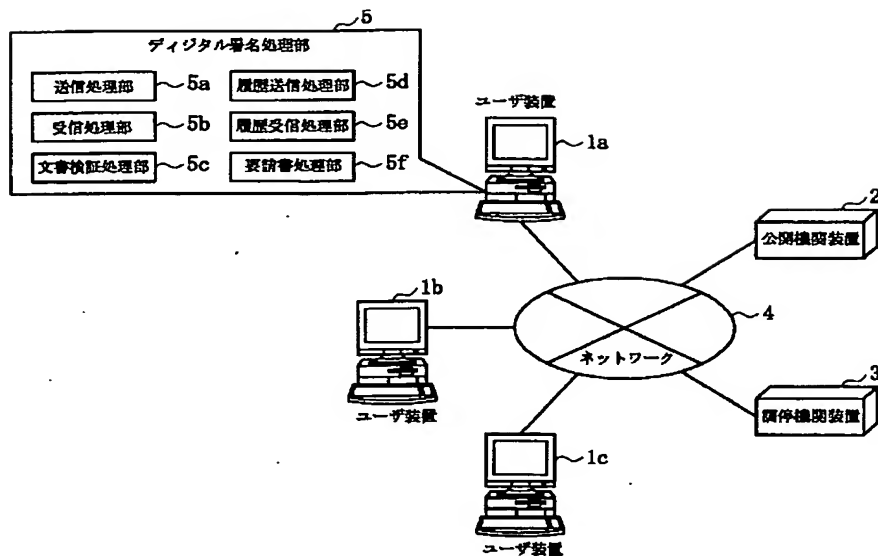
【図9】図2におけるユーザ装置の要請書処理プログラムに基づく処理動作例を示すフローチャートである。

【図10】本発明に係わるデジタル署名システムの処理動作の具体例を示す説明図である。

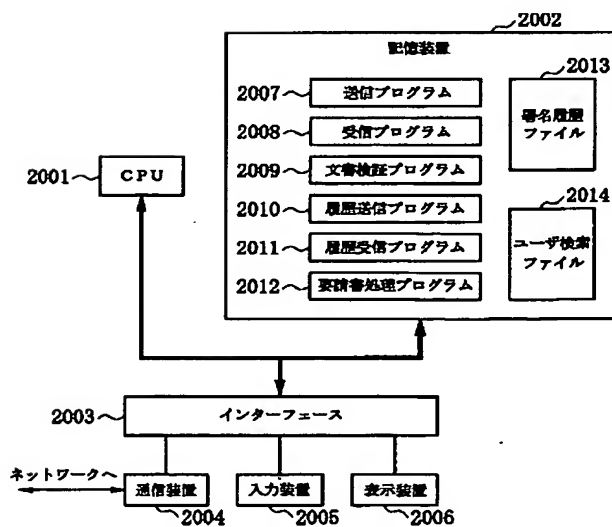
【符号の説明】

1a～1c：ユーザ装置、2：公開機関装置、3：調停機関装置、4：ネットワーク、2001：CPU、2002：記憶装置、2003：インターフェース、2004：通信装置、2005：入力装置、2006：表示装置、2007：送信プログラム、2008：受信プログラム、2009：文書検証プログラム、2010：履歴送信プログラム、2011：履歴受信プログラム、2012：要請書処理プログラム、2013：署名履歴ファイル、2014：ユーザ検索ファイル、3001～3003：レコード、3004：項目（「番号」）、3005：項目（「前回署名記録のハッシュ値」）、3006：項目（「文書のハッシュ値」）、3007：項目（「署名または相手の署名生成記録情報」）、3008～3010：レコード、3011：項目（「番号」）、3012：項目（「送受信符号」）、3013：項目（「相手情報」）、10001：ユーザ装置Aの署名履歴、10002：ユーザ装置Aのユーザ検索ファイル、10003：要請書、10004：ユーザ装置Bのユーザ検索ファイル、10005：ユーザ装置Bの署名履歴。

【図1】



【図2】



【図3】

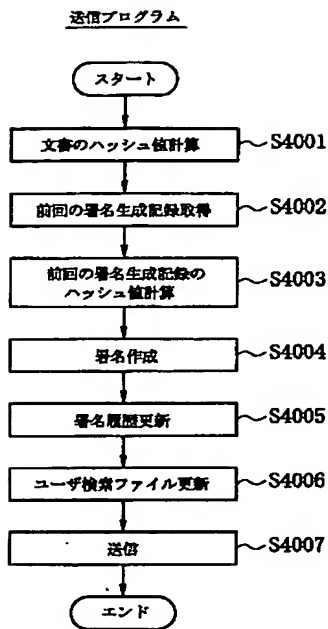
(a)

	3004	3005	3006	3007
	番号	前回署名記録のハッシュ値	文書のハッシュ値	署名or相手の署名生成記録情報
3001	1	H(S ₀)	H(M ₁)	Sign(1 H(S ₀) H(M ₁))
3002	2	H(S ₁)	—	32 H(S ₂₂)
3003	3	H(S ₂)	H(M ₃)	Sign(3 H(S ₂) H(M ₃))

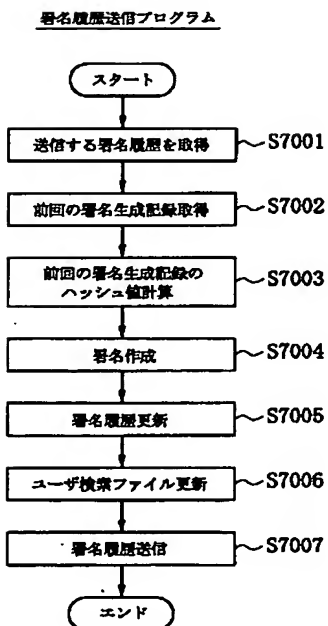
(b)

	3011	3012	3013
	番号	送受信符号	相手情報
3008	1	送信	kunthiko@AAA.co.jp
3009	2	受信	s-itoh@BBB.co.jp
3010	3	送信	tanimoto@CCC.co.jp

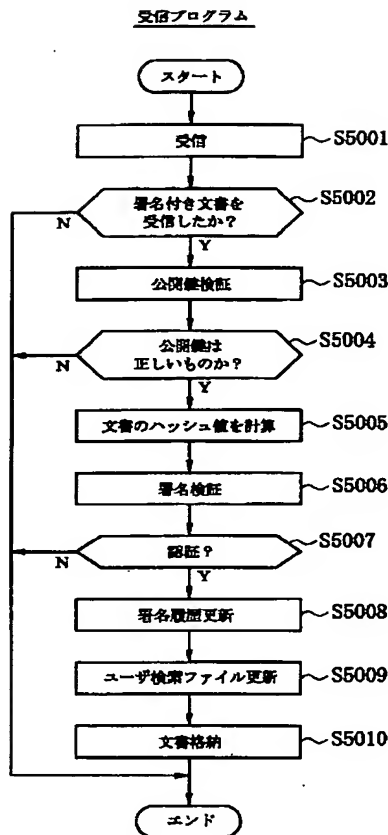
【図 4】



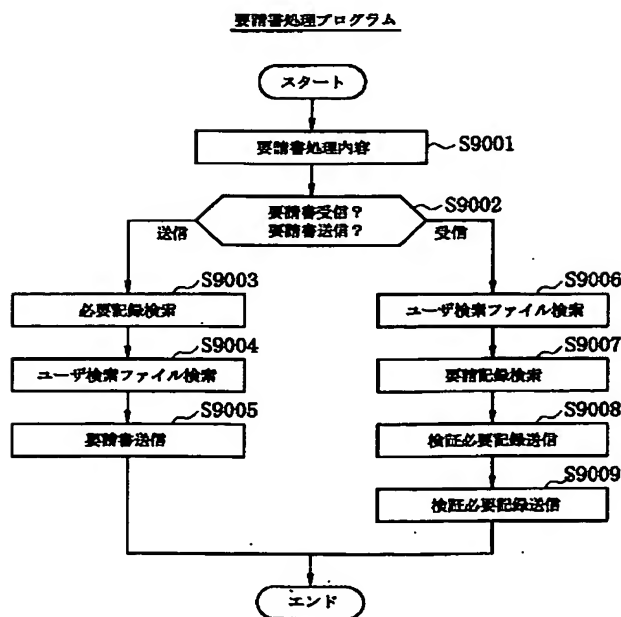
【図 7】



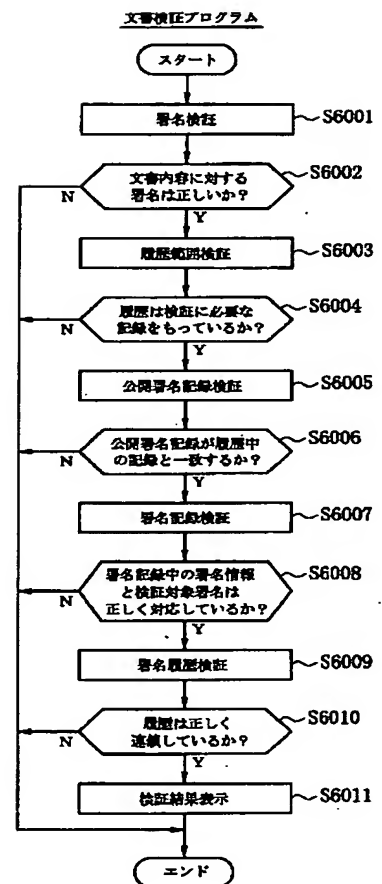
【図 5】



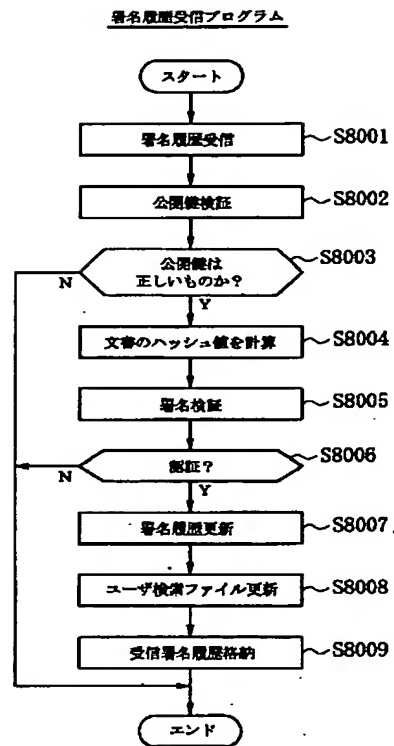
【図 9】



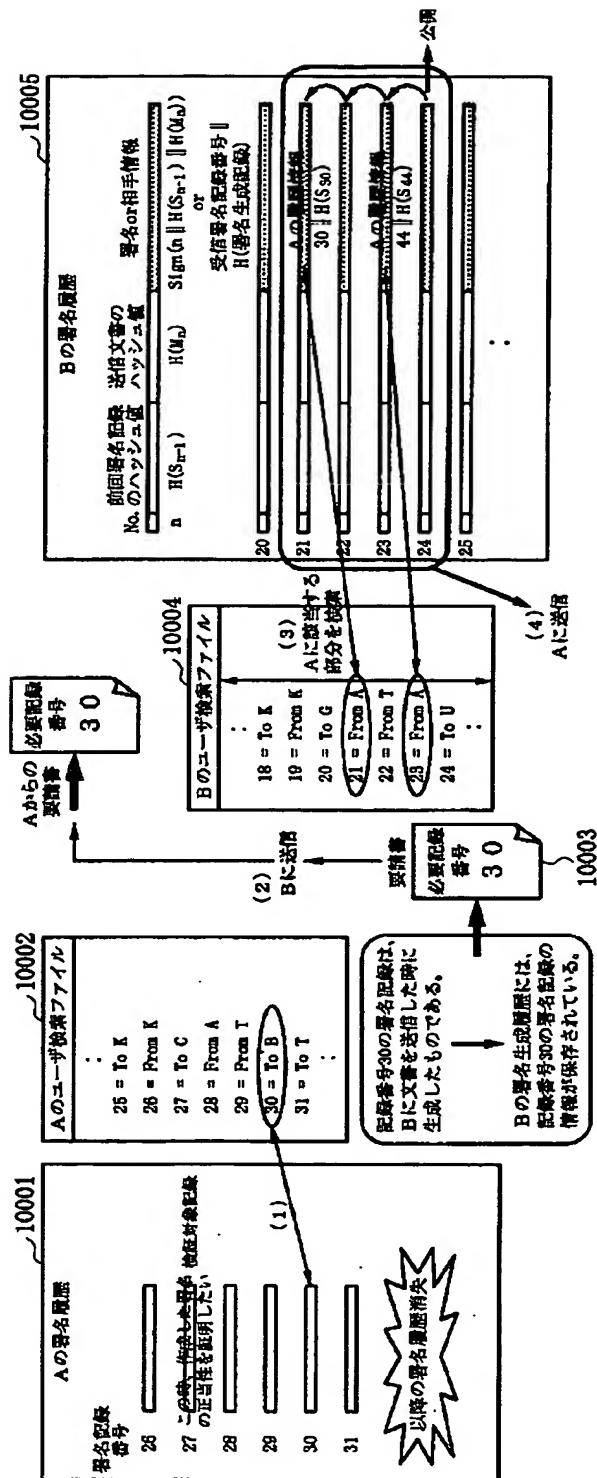
【図 6】



【図8】



【図10】



フロントページの続き

(72)発明者 宮崎 邦彦
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内
(72)発明者 大本 周広
東京都江東区新砂一丁目6番27号 株式会
社日立製作所公共システム事業部内

(72)発明者 西岡 佳津子
東京都江東区新砂一丁目6番27号 株式会
社日立製作所公共システム事業部内
Fターム(参考) 5J104 AA07 EA19 KA01 KA03 LA03
LA06 NA12 PA07 PA10